UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
	:	
- v -	:	
	:	**18 Cr. 81 (DLC)**
LAVELLOUS PURCELL,	:	
Defendant.	:	

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT LAVELLOUS PURCELL'S MOTION TO SUPPRESS EVIDENCE

Federal Defenders of New York
Attorneys for Defendant
Lavellous Purcell
52 Duane Street - 10th Floor
New York, NY 10007
Tel.: (212) 417-8734
Christopher A. Flood
Of Counsel

TO: Geoffrey S. Berman
United States Attorney
Southern District of New York
One St. Andrew's Plaza
New York, NY 10007
Attn: **AUSA Sheb Swett, Esq.**

TABLE OF AUTHORITIES

Cases

Statutes & Additional Authorities

PRELIMINARY STATEMENT

Lavellous Purcell opened a Facebook account in 2008 and used it thereafter to look up old friends and to keep connected with family. He communicated over the site's public platform, and also used its private messaging and location-based services.. By October, 2017, when the Government's impermissible access to his Facebook account concluded, Mr. Purcell's Facebook use had generated many thousands of pages of private information. The Government obtained this information through constitutionally-defective warrants issued in August 2016, November 2016, and September 2017. Mr. Purcell moves to suppress that evidence, and any other evidence that constitutes the fruits of the unconstitutional searches.

Additionally, the Government fails to sufficiently particularize its allegations beyond broad, categorical accusations regarding conduct alleged to have taken place outside the Southern District of New York. Mr. Purcell therefore seeks a bill of particulars identifying, among other things, the dates, locations, and particular nature of his alleged misconduct to aid him in determining whether the five-count indictment is duplicative or multiplicative, to evaluate whether venue is proper, and in preparing for his defense and avoiding surprise at trial.

First, in August, 2016, without a lawful or jurisdictional basis, the Government sought and obtained a search warrant ("August warrant") from a New York criminal trial court by which it obtained what amounts to the entire historical contents of Mr. Purcell's Facebook account. Despite the well-settled requirement of particularity for search warrants, the warrant itself wholly fails to identify or specifically incorporate any suspected crime, or the time period at issue. Rather, the warrant commands Facebook, Inc. to search twenty-four expansive categories of generic, electronically stored information ("ESI") to find evidence of "an offense." It further authorizes the Government to seize and to search everything Facebook, Inc. produces.

The list of ESI to be searched is so sweeping that it encompasses nearly every record associated with Mr. Purcell's account. It encompasses all records linked to Mr. Purcell's account (including those created by other people), his physical location tracked by the site, his list of friends and family, and the often extensive membership lists for any groups with whom Mr. Purcell associates. As a result, even if the executing agents or Facebook, Inc. could somehow determine the offenses under investigation absent any statement of those offenses on the face of the warrant, the Government's search would still constitute an overbroad, non-particularized, and constitutionally impermissible "all-records search" that lacked sufficient probable cause.

The affidavit in support of the search warrant makes no allegation that Mr. Purcell's entire Facebook account was permeated by fraud or any other wide-reaching criminal act. Rather, the affidavit attaches exhibits showing less than ten isolated, ambiguous postings representing a miniscule fraction of account activity, each of which it alleges relates to prostitution or promoting prostitution. Nonetheless, the Government's proposed list of ESI to be seized seeks "any", "all", or "any and all" records for all but one of twenty-four broad, generic categories of information.

Second, state law does not authorize the August 2016, November 2016, or September 2017 warrants. The State of New York executed the warrants in California, outside the jurisdictional reach of the issuing New York criminal court. Facebook is incorporated in California, and its headquarters are in Santa Clara, California. The New York State constitution and statutorily-defined process for executing search warrants restrict the issuing criminal court's authority to issue search warrants to those to be executed in the State of New York. The State of New York neither obtained the warrant under Rule 41 of the Rules of Federal Criminal Procedure, nor sought any assistance from a California court to execute the warrant in that state.

Rather, the State of New York served the warrant directly on Facebook through an electronic portal maintained by the company in California. Since the issuing court lacked any jurisdiction to obtain records held outside New York or to otherwise command Facebook, Inc. to comply, the warrants are void.

Third, the warrants are not authorized by federal law, which allows Facebook, Inc. to produce the contents of otherwise-private ESI only upon a warrant issued by a court of competent jurisdiction, and according to state law. The warrant here contravened both New York statutory and constitutional limitations, and thus did not provide the requisite basis for authorization under federal law. To the extent that federal law does permit the Government to obtain private ESI without a warrant, it limits such disclosure to six categories of basic subscriber information, and *prohibits* disclosure of the contents of the type of ESI the Government obtained here.

The November 2016 and September 2017 warrants are virtually identical to the August 2016 warrant. Both subsequent warrants are similarly void under New York and federal law. Were they not, neither provides sufficient additional information to justify an all-records search. Standing alone, the subsequent applications do not cure the first defective August 2016 warrant. Rather, the infirmities of the first application taint both subsequent applications wherein the Government wholly attaches, incorporates, and principally relies upon the defective August 2016 application and warrant.

Each of these constitutional infirmities, whether in an application or warrant itself, prevents the Government's good-faith reliance upon any warrant it obtained and calls for suppression of the evidence seized and the fruits thereof.

Fifth, Mr. Purcell also seeks a bill of particulars to prepare his defense and avoid surprise at trial. He stands accused of five different counts of violating federal law related to promoting prostitution, spanning a six-year period beginning in 2012, involving an unknown number of complaining witnesses. *See* Declaration of Christopher A. Flood ("Flood Decl.") ¶ 2 & Ex. A (Indictment).[1] Without the materials requested herein, it will be impossible for Mr. Purcell to comb the tens of thousands of pages documents, files, telephone records, and ESI produced by the Government to defend against these unspecified allegations. Accordingly, he respectfully requests that the Court order that the Government provide the requested particulars, which are necessary to (1) apprise him of the actual allegations against him, (2) determine before trial whether the indictment is duplicative or multiplicative, and (3) establish the propriety of venue in this district.

FACTUAL BACKGROUND

Mr. Purcell used a Facebook, Inc. account under the name Mike Hill. He registered it in his own name, and used it as a means of private communication for years. He never authorized law enforcement to access this account, and expected that Facebook, Inc. would keep its private contents private. (Ex. B, Purcell Declaration).

On August 5, 2016, pursuant to New York C.P.L. 690 and 18 U.S.C. § 2703 ("Electronic Communications Act"), and based on the sworn affidavit of a Senior Investigator with the New York County District Attorney's office (Ex. C), the Supreme Court of the City of New York County ordered Facebook, Inc. to search the contents of two accounts. (Ex. D). One of them

[1] All exhibits referenced herein are appended to the Flood Declaration.

belonged to Mr. Purcell. (Ex. B). Mr. Purcell opened, used, and had a reasonable expectation in the private contents of the "Hill" account. *Id*.

The August 2016 warrant commands Facebook, Inc. to perform a nearly unlimited, general search of the Hill account. The warrant also authorized a temporally limited search for another account that Mr. Purcell was alleged to be associated (the "Monroe" account). The warrant was served on Facebook, Inc. the same day as it was issued, August, 5, 2017. It directs Facebook to compile twenty-four separate categories of ESI from the Hill account, to analyze it, and to produce that which it concludes is "evidence of an offense." But the warrant neither specifies a specific offense, nor does it incorporate the supporting factual affidavit.[2] (Ex. D).

In response to the August 2016 warrant, Facebook, Inc. produced 180 days of records for both the Monroe account and the Hill account, limiting production for both accounts to the temporal limitation that the warrant had specified only for the "Monroe" account. Except as to the IP logs, however, the August 2016 warrant never specified a temporal limitation for the Hill account. (Ex.D). On November 1, 2016, the District Attorney's Office therefore sought a second search warrant for the Hill account. (Ex's. E & F). The application for the November 2016 warrant attached and incorporated the application for the previous warrant, but incorrectly states that the August 2016 warrant requested only twelve months of records for the Hill account. (Ex. E). The August 2016 warrant had only imposed such limitation on the IP logs from the Hill

[2] The issuing court also authorized a search of a Gmail account allegedly associated with Mr. Purcell, and associated bank records, based on a similar affidavit by the same Senior Investigator. The Government represents this warrant was served on Google, Inc. on August 5, 2016 and that Google, Inc. produced no responsive materials. Based on the Government's representations that no evidence was returned by the Gmail warrants, Mr. Purcell has no motion to suppress the fruits of those warrants.

account. There was no other temporal limitation applied to a search of that account. (Ex's C & E).

Ten months later, on September 26, 2017, the District Attorney's office sought a third warrant for the Hill account. (Ex's G & H). This affidavit relied on information obtained from both the August 2016 and November 2016 warrants, and incorporated the August 2016 warrant and warrant application. (Ex. G). Based on this affidavit, the court issued a third warrant on September 26, 2017. This warrant authorized a search of the Hill account through the issuance of the warrant. (Ex H). It was served on Facebook on September 26, 2017.

The Government provided confirmation from Facebook, Inc. that the dates of service cited here are accurate. The date of service is important for several reasons. New York law requires a warrant to be executed not more than ten days of authorization. N.Y. C.P.L. § 690.30(1). And also because Facebook's search of Mr. Purcell's account without notice to Mr. Purcell must be authorized by 18 U.S.C. 2703(b)(1)(A). Here, Facebook appears to have conducted at least three separate searches of Mr. Purcell's account in September and October of 2017. Only the last search generated results corresponding with the authorization of all the warrants *together*, but no search result corresponds to any individual warrant's authorized range of dates. (Ex. J) (Report generated on September 7, 2017 for date range August 1, 2015 to September 7, 2017; report generated on September 14, 2017 for date range September 6, 2016 to September 1, 2017; report generated on October 13, 2017 for date range August 1, 2015 to September 26, 2017). [3]

ARGUMENT

The evidence obtained from Mr. Purcell's Facebook account must be suppressed because it was obtained in violation of the Fourth Amendment to the United States Constitution. The evidence was obtained pursuant to warrants that are not authorized under state or federal law, and exceeds the scope of material obtainable through any other means than by valid search warrant. Because the warrants are invalid, at most, they authorize the Government to obtain limited categories of subscriber account information as specified in 18 U.S.C.A. § 2703(c)(2). Because the Government flagrantly violated the terms of these orders, the evidence obtained by them must be suppressed.

I. The Search of Mr. Purcell's Facebook Was Unreasonable

A. Searching the contents of a Facebook account requires a valid warrant.

Facebook provides a social media platform for broadcasting information to the public, but it also provides services for private communication between users. By adjusting the site's privacy settings, users can narrow the audience to whom their profile information and posting

[3] The Government provided confirmation from Facebook, Inc. that the dates of service cited here are accurate. The date of service is important for several reasons. New York law requires a warrant to be executed not more than ten days of authorization. N.Y. C.P.L. § 690.30(1). And also because Facebook's search of Mr. Purcell's account without notice to Mr. Purcell must be authorized by 18 U.S.C. 2703(b)(1)(A). Here, Facebook appears to have conducted at least three separate searches of Mr. Purcell's account in September and October of 2017. Only the last search generated results corresponding with the authorization of all the warrants together, but no search result corresponds to any individual warrant's authorized range of dates. (Ex. J) (Report generated on September 7, 2017 for date range August 1, 2015 to September 7, 2017; report generated on September 14, 2017 for date range September 6, 2016 to September 1, 2017; report generated on October 13, 2017 for date range August 1, 2015 to September 26, 2017).

are visible[4], and can use the site's "messenger" to communicate in private.[4] Postings using such "secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected."[5] The Second Circuit acknowledged the "potent threat to privacy" that a general search of such Governmental access to such content constitutes a search for purposes of the Fourth Amendment.[6]. In upholding a reasonable expectation of privacy in these communications, the court has required a valid warrant for searches of the content of these messages. *Ulbricht* at 97; *see also Carpenter v. United States*, 138 S.Ct. 2206, 2216 (2018) (confidential communications generally require a warrant). The returns from the warrants in this case provided the Government the private contents of Mr. Purcell's account, including private communications from his "Groups", private messages, and "pokes." *See e.g.* Ex. J.

Facebook protects the privacy of messages and chats in two ways.[7] First and foremost, a user must "approve" another user by "friending" them or by accepting their "connection request" in order to exchange private messages.[8] Second, Facebook alerts customers that "only you and the people you're messaging can view your conversation."[9] Like messages, "pokes" can only be

---

[4] *See* Ex. I "How can I adjust my privacy settings?", https://www.facebook.com/help/193677450678703?helpref=related, *last accessed August 4, 2018*.
[5] *See* Ex. J "Who can see my Facebook messages?" https://www.facebook.com/help/212388195458335?helpref=uf_permalink, *last accessed August 4, 2018*.
[6] *United States v. Meregildo*, 883 F. Supp 2d 523 (S.D.N.Y. 2012) (internal citation omitted); *aff'd, United States v. Pierce*, 785 F.3d 832 (2d Cir. 2015).
[7] *See United States v. Ulbricht*, 858 F.3d 71 (2d Cir. 2017) ("a general search of electronic data is an especially potent threat to privacy because hard drives and e-mail accounts may be akin to a residence in terms of the scope and quantity of private information [they] may contain"); *and United States v. Galpin*, 720 F.3d 436 (2d Cir. 2013) ("advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain").
[8] *See* "View and Manage Messages," https://www.facebook.com/help/111703937833429 9/?helpref=hc_fnav.
[9] *Id.*
[10] *Id.*

seen by the two parties engaging in the interaction.[10] Similarly, Facebook "Groups" have specific privacy settings, usually set by the group's administrators; while a group may be public, a group may also be "private," meaning that only those members admitted by administrators are able to see the existence of the "Group" or identify the other members.[11] By choosing to engage in private interactions with other individuals via chat, messenger, pokes and group participation, Mr. Purcell exhibited a clear "subjective expectation of privacy." *Katz v. United States,* 389 U.S 347, 361 (1967) (Harlan, J., concurring). The Second Circuit has held that this expectation is one "that society is prepared to recognize as reasonable." *Id*; *see also Meregildo,* 883 F. Supp 2d 523.

B. The Government May Only Obtain Location Information by Valid Warrant

The Supreme Court recently affirmed that an individual retains a legitimate privacy interest in "the record of his physical movements." *Carpenter,* 138 S.Ct. at 2218. Examining an individual's privacy interest in the context of retrospective cell-site location information ("CLSI"), the Court held "when the Government accessed CSLI from the wireless carriers, it invaded [the defendant's] reasonable expectation of privacy in the whole of his physical movements." *Id*. at 2219. The court specifically noted the breadth of the information provided by CLSI. *Id.* "[T]he retrospective quality of the data here gives police access to a category of information otherwise unknowable." *Id.* The Court clearly distinguished personal location data from cases in which it had applied the third-party doctrine to affirm a warrantless search of other records. *Id.* "These location records hold for many Americans the privacies of life." *Id*. at 2218 (internal citations and quotations omitted). Holding that access to CLSI constituted a search for

[11] *Id.*

[12] *See* "Group Privacy," https://www.facebook.com/help/1686671141596230/?helpref=hc_fnav.

purposes of the Fourth Amendment, the court held that "the Government must generally obtain a warrant supported by probable cause before acquiring such records." *Id.* at 2221.

A valid warrant was also required for the extensive retrospective location information the Government sought from Facebook, Inc. Specifically, the Government sought photos in which Mr. Purcell had been tagged, his "check-in" records, his "events" records, and his "update location" records. (Ex's. C, E, & G). This type of location information is similar to the CLSI considered in *Carpenter* in that it reveals the user's retrospective location information, including the Global Positioning System (GPS) data showing the user's precise geographical location. Further, it may be accessed through a cellphone and can be revealed without approval of that user. *See Terms of Service, Facebook.com,* https://www.facebook.com/terms.php (last visited Aug. 6, 2018).The data provides retrospective location data by showing the precise location (establishment or residence) where the "check-in" or "tag" has occurred. *Id.* As most cell phones can access Facebook through either the internet or the Facebook app, this "tag" or "check-in" can occur on a cellphone, a device that the Supreme Court noted in *Carpenter* cannot be automatically subjected to the third-party doctrine because "carrying one is indispensable to participation in modern society." *Carpenter*, 138 S.Ct. at 2220. The Court further emphasized the involuntary nature of location sharing through CLSI, noting that a user's location could be shared "without any affirmative act on the part of the user." *Id.* Like CLSI, location sharing via Facebook is not always a voluntary act, as a user can be "tagged" at a location or "check-in" by another user without consent. *Id*. This type of location information, in short, implicates the same privacy concerns at issue in *Carpenter* and generally may be obtained only by valid warrant.

C. The Insufficiently Particular, Invalid Warrants Cannot Justify the Search in this Case.

The Second Circuit has long held that insufficient particularity renders a warrant invalid. "First, a warrant must identify the specific offense for which the police have established probable cause. Second, a warrant must describe the place to be searched. Third, the warrant must specify the items to be seized by their relation to designated crimes." *United States v. Galpin*, 720 F.3d 436 (2d Cir. 2013); *see also United States v. George*, 975 F. 2d 72 (2d Cir. 1992) (warrant insufficiently broad absent statement of alleged crime); *United States v. Young*, 745 F. 2d 733 (2d Cir. 1984) (same).

While the Second Circuit has permitted the Government to obtain the entire contents of a computer hard drive, social media account or email account by valid warrant, it has required that the actual *search* of that material be limited to material responsive to the probable cause showing in the warrant. *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016). Addressing the same issue in the context of a Gmail account, the Southern District of New York affirmed the ability of the government to "access an entire email account in order to conduct a search for emails *within the limited categories contained in the warrant*." *In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc.*, 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014), as amended (Aug. 7, 2014) (emphasis added).

Additionally, temporal limitations in searches of electronic communications are relevant to particularity analysis. *See United States v. Wey*, 256 F.Supp.3d 355 (S.D.N.Y 2017) (finding a warrant to lack particularity in part because of insufficient temporal limitations); *United States v. Zemlyansky*, 945 F.Supp. 2d 438, 459 (S.D.N.Y. 2013) ("[A] warrant's failure to include a time limitation, where such limiting information is available and the warrant is otherwise wide-

ranging, may render it insufficiently particular"); *see also United States v. Jacobson*, 4 F. Supp. 3d 515 (E.D.N.Y. 2014) ("[A] warrant's failure to include a temporal limitation on the things to be seized may, in certain circumstances, render a warrant insufficiently particular").

A sufficiently particularized warrant *application* does not cure a deficiently particular warrant unless it explicitly is incorporated into the warrant. "Resort to an affidavit to remedy a warrant's lack of particularity is only available when it is incorporated by reference in the warrant itself." *George*, 975 F.2d at 76.; *see also Groh v. Ramirez*, 540 U.S. 551 124 S.Ct. 1284 (2004) (holding that Fourth Amendment requires particularity in the warrant not supporting documents). Courts have required warrants to clearly cite to and incorporate an attached affidavit. *See George*, 975 F.2d 72 (2d Cir. 1992) ("[t]he recitation in the instant warrant that it is "issued upon the basis of an application and affidavit of Patrolman Brickell does not direct the executing officers to refer to the affidavit for guidance concerning the scope of the search and hence does not amount to incorporation by reference") (internal alteration omitted).

1. The August 2016 Warrant.

The August 2016 warrant itself identifies no criminal charge whatsoever. (Ex. D). Rather, it merely states that there is probable cause to believe the account contains evidence of "an offense" *Id*. Unsurprisingly, perhaps, given this overbroad authorization, the warrant fails to connect the extensive list of broad categories of generic ESI to an offense under investigation. *Id*. Additionally, while the August 2016 warrant specifies a temporal limitation for IP log information from the Hill account, it does not specify a temporal limitation for any of the other categories of information. Finally, the warrant fails to incorporate the underlying affidavit as is

required by the Second Circuit, and merely states that an affidavit has been sworn, similar to the warrant held insufficient in *George*.

2. The November 2016 Warrant.

The November 2016 application wholly incorporates the previous, August 2016 application, and adds additional, recently-posted exhibits that do not qualitatively alter the probable cause analysis. (Ex. E). The November 2016 warrant states alleged offenses, but to relate the probable cause for the search to the extensive categories of information sought from Mr. Purcell's Facebook account. (Ex. F). It cites the supporting affidavit only inasmuch as the warrant merely states that "proof has been sworn by affidavit" and therefore cannot incorporate that document. *Id.* Further, the November 2016 warrant sets fails to set any temporal limitation for the Hill account except as to the IP logs, which it authorizes from "8/1/15 through the date of this warrant." *Id.*

3. The September 2017 Warrant.

The September 2017 application relies on information illegally obtained as a result of the unreasonable August search: "Information obtained through [the search based on the August 2016 order] confirmed that "Mike Hill," the user of the target account, used the target account to send private messages to numerous female individuals." (Ex. G at ¶ 5(h)). It makes no reference to the November 2016 application or warrant, but attaches additional exhibits, one of which is the entire August 2016 application.

Replicating the August 2016 warrant verbatim, the September 2017 warrant entirely fails to specify any specific crime, but only "an offense." It also fails to incorporate the supporting affidavit, or to link the probable cause showing to any of twenty-four categories of ESI it

authorizes to be searched, and fails to temporally limit the search for any category except the IP logs and most recent check in data.

II. The Orders Do Not Constitute Warrants Under State Law

The Government cannot obtain the information from Mr. Purcell's private Facebook communications without a valid state or federal warrant. 18 U.S.C.A. 2703 (a). Issued under New York State Law, (Ex's. D, F, & H (caption)) each warrant violated the geographic jurisdictional restriction established in Article 6, section 1 of the Constitution of the State of New York, and implemented under of New York Criminal Procedure Law § 690.20(2) (McKinney 2018). Under the clear terms of that statute, the warrants could be executed only in "a county of issuance or an adjoining county" in New York state. *Id.* "[T]he government points to no authority to suggest that a county judge in New York has the authority under New York law to issue a warrant authorizing a search in another state." *U.S. v. Ramsey, 2:14-CR-00296,* 2017 WL 1349185, at *11 (E.D. Pa. Mar. 7, 2017); *see also People v. Hickey,* 40 N.Y.2d 761, 763 (1976) (holding "[w]here the underlying offense allegedly occurred within the geographic jurisdiction of the Justice Court, a search warrant may, if necessary, be executed throughout the county or in an adjoining county); *United States. v. Gotti,* 42 F. Supp. 2d 252, 286 (S.D.N.Y. 1999) (same).

The warrants in this case were served on Facebook at its headquarters in Santa Clara, California by New York State Law enforcement. (Ex's. D, F, & H). They were uploaded via an electronic portal; there is no indication that a California court of jurisdiction was involved or that the warrants themselves were executed by California law enforcement. *Id.* As New York state warrants can only be executed in the county of issuance or a surrounding county, the warrants do not constitute valid warrants outside of New York State.

III. 18 U.S.C § 2703 Does Not Authorize the Warrants.

A. Federal law authorizes search of a Facebook account only by valid warrant.

Federal law prevents the disclosure of the contents of electronically stored information without a valid warrant "issued pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, *issued using State warrant procedures*) by a court of competent jurisdiction." 18 U.S.C. § 2703(a) (emphasis added). Neither of the statute's dual requirements as to State court warrants was followed here. As it was directed to and served beyond the borders of New York, the warrant was issued in violation of C.P.L § 690.20. Section 2703 cannot authorize the warrant because the issuing New York court lacked competent jurisdiction to order the search of ESI held in California.

Section 2703(b) authorizes a "government entity" to "require a provider of remote computing service to disclose the contents" of electronic communications without notice to the subscriber. 18 U.S.C. § 2703(b). But even if this section were to apply, it also requires the government entity to "obtain a warrant", and where such a warrant is not obtained under the Federal Rules of Criminal Procedure, it must be "issued using State court warrant procedures", which, as discussed above, were not followed here. As with § 2703(a), § 2703(b) requires the warrant to be issued "by a court of competent jurisdiction." *Id.* Federal law therefore does not authorize the search Mr. Purcell's Facebook account.

B. Absent a valid warrant, the Government was permitted to obtain a very limited category of electronic communications under 18 U.S.C.A. § 2703.

Section 2703 authorizes the Government to obtain a limited set of electronic communications without a valid warrant. The Government "may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication…if the governmental entity 1) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or obtains a court order

for such disclosure under subsection (d) of this section." 18 U.S.C.A. § 2703(c). However, by subpoena, the government may only require disclosure of a limited category of information. *Id.* Absent a valid state or federal warrant, the government may require disclosure of the "(A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number) of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury." *Id.*

Without a valid warrant, the Government would not be permitted to obtain the contents of any of messages, chats, emails or drafts, Mr. Purcell's location information or his list of contacts on either service provider. The warrants were not valid under state law, therefore anything outside the bounds of the information authorized in the categories specified by 18 U.S.C. § 2703 must be suppressed.

IV. Bill of Particulars

The Second Circuit has held that a defendant is entitled to a bill of particulars, pursuant to Rule 7(f) of the Federal Rules of Criminal Procedure, when an indictment (or alternate document) does not sufficiently provide particularity of the nature of the alleged charge. *United States v. Bortnovsky*, 820 F.2d 572 (2d Cir. 1987). In determining whether to grant the motion for a bill of particulars, courts are compelled to "examine the totality of the information available to the defendant—through the indictment, affirmations, and general pre-trial discovery." *United States v. Bin Laden*, 92 F. Supp. 2d 225, 233 (S.D.N.Y. 2000), aff'd sub nom. *In re Terrorist*

Bombings of U.S. Embassies in E. Africa, 552 F.3d 93 (2d Cir. 2008). Courts have denied the motion in cases where 1) the indictment is sufficiently specific regarding the nature, time frame and location of the charges or 2) where the government had made "sufficient disclosures concerning its evidence and witnesses by other means." *United States v. Chen*, 378 F.3d 151 (2d Cir. 2004). Additionally, courts have held that in certain cases "the large volume of material disclosed is precisely what necessitates a bill of particulars." *Id.* at 234; *see also Bortnovsky*, 820 F.2d 572 ("[defendants] were forced to explain the events surrounding eight actual burglaries and to confront numerous documents unrelated to the charges pending. In effect, the burden of proof impermissibly was shifted to [defendants]"); *United States v. Nachamie*, 91 JF. Supp. 2d 565 (S.D.N.Y. 2000) ("[b]ecause the Government has declined to identify which of the documents provided to the defense pursuant to Rule 16(a)(1)(C) it intends to use in its case-in-chief at trial, it must, instead, respond to an appropriate bill of particulars").

In Mr. Purcell's case, the government has not sufficiently specified the nature, location and time frame of the alleged charges. The indictment alleges: violation of 18 U.S.C. § 2422 (a) based on allegations that Mr. Purcell "recruited women over the internet and in person to travel in interstate commerce" over a two-year period (emphasis added); violation of 18 U.S.C. § 2421 (a) based on allegations that Mr. Purcell "transported women to multiple states, including New York, with the intent that the women engage in prostitution" over a one year period; violation of 18 U.S.C. § 1952 (a) based on allegations that Mr. Purcell "used a cellular phone and the internet to promote, manage, establish, and carry on a criminal business engaged in prostitution"; violation of 18 U.S.C. § 1952 (a) (3) based on allegations that Mr. Purcell "did combine, conspire, confederate, and agree…to commit an offense against the United States" and between 2012 and 2016, in violation of 18 U.S.C. § 1591 (a)(1)(2) "knowingly recruited…and

maintained a person…in reckless disregard of the fact that means of force, threats of force, fraud, and coercion would be used to cause that person to engage in commercial sex acts." (Ex. A). It further specifies the overt act for the alleged conspiracy as 1) posting an advertisement on Backpage.com on a specified date "promoting prostitution" and 2) using a facility in interstate commerce to reserve a hotel room in Virginia "for the purposes of promoting prostitution" in violation of 18 U.S.C. § 371. *Id.*

No charge in the indictment alleges a date range of less than two years, specifies a location other than a single overt act alleged to have taken place in this district (accomplished by posting on Backpage.com), only describes the complainants by gender, does not specify or limit their number, or describes Mr. Purcell's alleged conduct in anything other than generic statutory language. Such broad allegations are insufficiently specific to allow Mr. Purcell to "prepare for trial, to prevent surprise, and to interpose a plea of double jeopardy should he be prosecuted a second time for the same offense." *Bortnovsky*, 820 F.2d at 574. Additionally, the Government produced extensive discovery without specifying which (1) calls, (2) emails, (3) backpage.com postings or (4) Facebook postings/messages would be used against Mr. Purcell, rendering him unable to adequately prepare for trial. *See Bin Laden*, 92 F. Supp. 2d 225, 236.

At minimum, without a Bill of Particulars, Mr. Purcell cannot discern whether the same conduct is charged in multiple counts, or whether multiple charges are improperly combined in one charged count. Because the indictment fails to particularize the location of the unspecified conduct, Mr. Purcell cannot determine whether venue is proper in the Southern District of New York.

CONCLUSION

For the reasons stated, and for any other the Court deems just and proper, Mr. Purcell's motions should be granted.

Dated: New York, New York
August 7, 2018

Respectfully submitted,
Federal Defenders of New York

By: 

Christopher A. Flood
Counsel for Lavellous Purcell
52 Duane Street - 10th Floor
New York, New York 10007
Tel.: (212) 417-8734